Nisqually Tribe

Information Technology Policy

Prepared by Nisqually Information Technology Division

Policy Approved by Tribal Administrator, Richard A. Wells 8/1/2006

Nisqually Tribe IT Acceptable Use Policy

1.0 Overview

Nisqually Tribe IT's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Nisqually Tribe's established culture of openness, trust and integrity. Nisqually Tribe IT is committed to protecting Nisqually Tribe's employees, partners and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly.
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Nisqually Tribe. These systems are to be used for business purposes in serving the interests of the organization, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.
Effective security is a team effort involving the participation and support of every Nisqually Tribe employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Nisqually Tribe. These rules are in place to protect the employee and Nisqually Tribe. Inappropriate use exposes Nisqually Tribe to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Nisqually Tribe, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Nisqually Tribe. These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

4.0 Policy

4.1 General Use and Ownership

1. While Nisqually Tribe's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Nisqually Tribe. Because of the need to protect Nisqually Tribe's network, management cannot guarantee the confidentiality of information stored on any network device belonging to outside entities.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. Nisqually Tribe IT recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Nisqually Tribe IT's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Nisqually Tribe IT's Awareness Initiative.

4. For security and network maintenance purposes, authorized individuals within Nisqually Tribe may monitor equipment, systems and network traffic at any time, per Nisqually Tribe IT's Audit Policy.
5. Nisqually Tribe reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by tribal confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: organization private, government strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K, XP users) when the host will be unattended.
4. Use encryption of information in compliance with Nisqually Tribe IT's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by employees from a Nisqually Tribe email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Nisqually Tribe , unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the Nisqually Tribe Internet/Intranet/Extranet, whether owned by the employee or Nisqually Tribe, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of Nisqually Tribe authorized to engage in any activity that is illegal under local, state, tribal, federal or international law while utilizing Nisqually Tribe-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the

installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Nisqually Tribe .

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Nisqually Tribe or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Nisqually Tribe computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Nisqually Tribe account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Nisqually Tribe IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Nisqually Tribe employees to parties outside Nisqually Tribe.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Nisqually Tribe 's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Nisqually Tribe or connected via Nisqually Tribe 's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History *8/1/2006*

These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Nisqually Tribe Email Use Policy

1.0 Purpose
To prevent tarnishing the public image of Nisqually Tribe When email goes out from Nisqually Tribe the general public will tend to view that message as an official policy statement from the Nisqually Tribe.

2.0 Scope
This policy covers appropriate use of any email sent from a Nisqually Tribe email address and applies to all employees, vendors, and agents operating on behalf of Nisqually Tribe.

3.0 Policy
3.1 Prohibited Use. The Nisqually Tribe email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Nisqually Tribe employee should report the matter to their supervisor immediately.

3.2 Personal Use.
Using a reasonable amount of Nisqually Tribe resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a Nisqually Tribe email account is prohibited. Virus or other malware warnings and mass mailings from Nisqually Tribe shall be approved by Nisqually Information Technology Director before sending. These restrictions also apply to the forwarding of mail received by a Nisqually Tribe employee.

3.3 Monitoring
Nisqually Tribe employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Nisqually Tribe may monitor messages without prior notice. Nisqually Tribe is not obliged to monitor email messages.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	Definition
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
Forwarded email	Email resent from an internal network to an outside point.
Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to Nisqually Tribe or its customers' reputation or social standing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside Nisqually Tribe, who do not have a need to know that information.

6.0 Revision History 8/1/2006
These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Policy Approved by Tribal Administrator, Richard A. Wells 8/1/2006

Automatically Forwarded Email Policy

1.0 Purpose
To prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope
This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Nisqually Tribe.

3.0 Policy
Employees must exercise utmost caution when sending any email from inside Nisqually Tribe to an outside network. Unless approved by an employee's supervisor, Nisqually Tribe email will not be automatically forwarded to an external destination. Sensitive information, as defined in the *Information Sensitivity Policy*, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with the *Acceptable Encryption Policy*.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Eudora and Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Nisqually Tribe or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Revision History 8/1/2006
These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Policy Approved by Tribal Administrator, Richard A. Wells 8/1/2006

Wireless Communication Policy

1.0 Purpose
This policy prohibits access to Nisqually Tribe networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Nisqually Tribe IT are approved for connectivity to Nisqually Tribe's networks.

2.0 Scope
This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Nisqually Tribe's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Nisqually Tribe's networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards
All wireless Access Points / Base Stations connected to the Nisqually Tribe network must be registered and approved by Nisqually Tribe IT. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in Nisqually Tribe laptop or desktop computers must be registered with Nisqually Tribe IT

3.2 Approved Technology
All wireless LAN access must use Nisqually Tribe-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication
All computers with wireless LAN devices must utilize a Nisqually Tribe-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

3.4 Setting the SSID
The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms	**Definitions**
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History
July 10, 2006, Section 3.4 Added
Final 8/1/2006
These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Policy Approved by Tribal Administrator, Richard A. Wells 8/1/2006

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Nisqually Tribe. Effective implementation of this policy will minimize unauthorized access to Nisqually Tribe proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by Nisqually Tribe, and to servers registered under any Nisqually Tribe-owned internal network domain.

This policy is specifically for equipment on the internal Nisqually Tribe network. For secure configuration of equipment external to Nisqually Tribe on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities
All internal servers deployed at Nisqually Tribe must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Nisqually Tribe Information Technology Division. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by Nisqually Tribe Information Technology Division.

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines
- Operating System configuration should be in accordance with approved Nisqually Tribe Information Technology Division guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to Nisqually Tribe Information Technology Division, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within Nisqually Tribe.
- Audits will be managed by the internal audit group or Nisqually Tribe Information Technology Division, in accordance with the *Audit Policy*. Nisqually Tribe Information Technology Division will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term	**Definition**
DMZ	De-militariezed Zone. A network segment external to the production network.
Server	For purposes of this policy, a Server is defined as an internal Nisqually Tribe Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History 8/1/2006

These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Nisqually Tribe Governmental Administration/Operation without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Nisqually Tribe Confidential information (e.g., Nisqually Tribe Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your supervisor. Questions about these guidelines should be addressed to Administration.

2.0 Scope

All Nisqually Tribe information is categorized into two main classifications:

- Nisqually Tribe Public
- Nisqually Tribe Confidential

Nisqually Tribe Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to the Nisqually Tribe.

Nisqually Tribe Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our Tribe. Also included in Nisqually Tribe Confidential is information that is less critical, such as telephone directories, general Govermental information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Nisqually Tribe Confidential information is "Nisqually Tribe Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Nisqually Tribe by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Nisqually Tribe's network to support our operations.

Nisqually Tribe personnel are encouraged to use common sense judgment in securing Nisqually Tribe Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Nisqually Tribe Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Nisqually Tribe Confidential information in question.

3.1 **Minimal Sensitivity:** General Government information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Nisqually Tribe Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Nisqually Tribe Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Nisqually Tribe information is presumed to be "Nisqually Tribe Confidential" unless expressly determined to be Nisqually Tribe Public information by a Nisqually Tribe employee with authority to do so.

Access: Nisqually Tribe employees, contractors, people with a business need to know.
Distribution within Nisqually Tribe: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Nisqually Tribe internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Nisqually Tribe premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Nisqually Tribe Confidential" or "Nisqually Tribe Proprietary", wish to label the information "Nisqually Tribe Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Nisqually Tribe employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Nisqually Tribe: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Nisqually Tribe internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Nisqually Tribe, but should be encrypted or sent via a private link to approved recipients outside of Nisqually Tribe premises.

Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on Nisqually Tribe premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our organization

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Nisqually Tribe Confidential information is very sensitive, you may should label the information "Nisqually Tribe Internal: Registered and Restricted", "Nisqually Tribe Eyes Only", "Nisqually Tribe Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Nisqually Tribe Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Nisqually Tribe employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Nisqually Tribe: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Nisqually Tribe internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within Nisqually Tribe, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Nisqually Tribe premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Terms and Definitions

Appropriate measures
To minimize risk to Nisqually Tribe from an outside business connection. Nisqually Tribe computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Nisqually Tribe Government information, the amount of information at risk is minimized.

Configuration of Nisqually Tribe-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Nisqually Tribe is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Nisqually Tribe.

Encryption
Secure Nisqually Tribe Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to Nisqually Tribe's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that Nisqually Tribe has control over it's entire distance. For example, all Nisqually Tribe networks are connected via a private link. A computer with

modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Nisqually Tribe also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Nisqually Tribe has established private links include all announced acquisitions and some short-term temporary links

6.0 Revision History 8/1/2006

These policies supersede all previous Information Technology policy and are designed in the best interest of the Nisqually Tribe.

Audit Vulnerability Scan Policy

1.0 Purpose
The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the Information Technology Division to the Nisqually Tribe. Information Technology Division shall utilize their own software to perform electronic scans of Client's networks and/or firewalls or on any system at Nisqually Tribe.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents ensure conformance to Nisqually Tribe security policies
- Monitor user or system activity where appropriate.

2.0 Scope
This policy covers all computer and communication devices owned or operated by Nisqually Tribe. This policy also covers any computer and communications device that are present on Nisqually Tribe premises, but which may not be owned or operated by Nisqually Tribe. The Information Technology Division will not perform Denial of Service activities.

3.0 Policy
When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of auditing organization. Nisqually Tribe hereby provides its consent to allow of Information Technology Division to access its networks and/or firewalls to the extent necessary to allow [Audit organization] to perform the scans authorized in this agreement. Nisqually Tribe shall provide protocols, addressing information, and network connections sufficient for Information Technology Division to utilize the software to perform network scanning.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Nisqually Tribe equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Nisqually Tribe networks.

3.1 Network Control.
If Client does not control their network and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing if scanning is to occur outside of the Nisqually Tribe LAN. By signing this agreement, all involved parties acknowledge that they authorize of Information Technology Division to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

3.2 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. Nisqually Tribe releases Information Technology Division of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result auditing organization's gross negligence or intentional misconduct.

3.3 Client Point of Contact During the Scanning Period. Nisqually Tribe shall identify in writing a person to be available if the result Information Technology Division Scanning Team has questions regarding data discovered or requires assistance.

3.4 Scanning period. Nisqually Tribe and Information Technology Division Scanning Team shall identify in writing the allowable dates for the scan to take place.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History
1/1/ 2006, updated to include National Association of State Auditors, Comptrollers, and Treasurers; the National Association of Local Government Auditors; the U.S. General Accounting Office; and U.S. Inspectors General Legal and Reporting Considerations.

CERTIFICATION

We certify that the foregoing policy was adopted at a regular meeting of the Nisqually Tribal Council held on _____, that a quorum was present, and that the policy was adopted by a vote of ___ FOR, ___AGAINST, and ___ ABSTAINING.

ATTEST

_____
Cynthia Iyall, Chairperson
NISQUALLY INDIAN TRIBE

_____
Norine L. Wells, Secretary
NISQUALLY INDIAN TRIBE